O

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

SECURED MAIL SOLUTIONS, LLC,
Plaintiff,
vs.

ADVANCED IMAGE DIRECT LLC, ET AL.,
Defendants.

Case No.: SACV 12-01090 DOC(RNBx)

FINAL ORDER ON CLAIM CONSTRUCTION

Before the Court are Plaintiff's Motion for Summary Judgment of Infringement (Dkt. 139) and Motion for Summary Judgment of Validity (Dkt. 138) and Defendants' Motion for Summary Judgment of Non-infringement (Dkt. 143). The parties simultaneously briefed claim construction issues. The Court considers only the claim construction issues at this time, and will issue a separate ruling on the motions for summary judgment on infringement and validity.

I. Background

This lawsuit addresses software tools designed to aid in large-scale commercial mailings. Defendants Envelopes Unlimited ("EU") and Advanced Image Direct ("AID") produce and send mailings on behalf of their clients. Clients give AID and EU the content and design of the mailing the client wishes to send and the mailing information for where the client wants the mailings sent. EU and AID print and send the mailings using specialized software and processes that qualify for specific discounts from the United States Postal Service ("USPS").

Plaintiff Secured Mail Solutions ("SMS") claims that Defendants are infringing on its method and system patents that set out a way of assigning specific identifying information to pieces of mail and then using post office data to verify that information. Some of the allegedly infringing processes are performed by a third party, GrayHair, which is not named in this lawsuit. EU and AID use GrayHair's software (a primary program called GHSelect and an add-on called SelectTrak) to assign identifying information to and track mailings. SMS claims that EU and AID are liable for infringement performed in part by GrayHair.

The parties briefed and argued their *Markman* and dispositive motion issues. This order constitutes the Court's final ruling on claim construction.

a. Patents at Issue

This case centers on a series of patents that issued from a provisional application filed on October 16, 2011. *See* Fitzsimmons Decl. Ex. A-1. Three are relevant to this litigation: U.S. Patent No. 7,814,032 (the "'032 Patent"), U.S. Patent No. 7,818,268 (the "'268 Patent"), and U.S. Patent No. 8,073,787 (the "'787 Patent"). Only claims in the '268 and '787 Patents remain at issue in the lawsuit. These patents are similar and share much overlapping language. Both address methods of using encoded data on the outside of mail pieces to verify or authenticate those mail pieces.

The inventor and president of SMS, Todd Fitzsimmons, developed the idea for this series of patents after the events of September 11, 2011. Fitzsimmons Decl. ¶ 5. Mr. Fitzsimmons imagined that the patented system could protect mail recipients from possible anthrax or explosive attacks by mail because the system would permit recipients to verify the source of the package before opening it. *Id*. ¶¶ 5-8.

b. Claims at Issue

Plaintiff alleges that Defendants infringe the following claims in the ‘268 Patent:

<u>Claim 1</u>

1. A method of verifying mail identification data, comprising:

> Affixing mail identification data to at least one mail object, said mail identification data comprising a single set of encoded data that includes at least a unique identifier, sender data, recipient data and shipping method data, wherein said unique identifier consists of a numeric value assigned by a sender of said at least one mail object.
>
> Storing at least a verifying portion of said mail identification data;
>
> Receiving by a computer at least an authenticating portion of said mail identification data from at least one reception device via a network, wherein said authenticating portion of said mail identification data comprises at least said sender data and said shipping method data; and
>
> Providing by said computer mail verification data via said network when said authenticating portion of said mail identification data corresponds with said verifying portion of said mail identification data.

See ‘268 Patent 6:18-37.

<u>Claim 1 Dependent Claims:</u>

5. The method of claim 1, wherein said step of receiving at least an authenticating portion of said mail identification data further comprises receiving at least said authenticating portion of said mail identification data from said at least one reception device via said network, wherein said authenticating portion of said mail identification data further comprises at least said unique identifier.

9. The method of claim 1, wherein said step of receiving at least an authenticating portion of said mail identification data further comprises receiving at least said authenticating portion of said mail identification data from said at least one reception device via said

network, wherein said authenticating portion of said mail identification data further comprises at least said recipient data.

See ‘268 Patent 6:49-55, 7:1-7.

Claim 33

33. A mail verification system for authenticating at least one mail object, said at least one mail object being a physical object and including mail identification data, comprising:

At least one mail verification device adapted to communicate with at least one reception device via a network, said at least one mail verification device comprising:

A memory, and

A mail verification application adapted to:

Store at least a verifying portion of mail identification data in said memory, said mail identification data comprising a single set of encoded data that includes at least a unique identifier, sender information, recipient information and shipping method information, wherein said unique identifier consists of a numeric value assigned by a sender of said at least one mail object;

Receive at least an authenticating portion of said mail identification data from said at least one reception device via said network, wherein said authenticating portion comprises at least said sender information and said shipping method information; and

Provide mail verification data via said network if at least said authenticating portion of said mail identification data corresponds to said verifying portion of said mail identification data.

See ‘268 Patent 8:62-9:19.

Claim 33 dependent claims:

39. The mail verification system of claim 33, wherein said authenticating portion of said mail identification data further includes at least said unique identifier.

40. The mail verification system of claim 39, wherein said authenticating portion of said mail identification data further includes at least said recipient information.

See ‘268 Patent 9:38-43.

Plaintiff alleges that Defendants infringe the following claims in the ‘787 Patent:

Claim 1

1. A system for authenticating a mail object, said mail object being provided to a mail carrier and including mail identification data affixed on said mail object in a single barcode, comprising:

first computer configured to communicate at least a first portion of said mail identification data over a network, said mail identification data including a shipping portion, a recipient portion, a sender portion, and an identifier portion, wherein said shipping portion includes shipping method data, said recipient portion includes an address of a recipient of said mail object, and said identifier portion includes a unique identifier that consists of a numeric value assigned by a sender of said mail object;

a database; and

a second computer comprising a verification application, said second computer being configured to receive at least said first portion of said mail identification data from said first computer via said network, said first portion of said mail identification data consisting of said shipping portion, said sender portion and said identifier portion;

wherein said verification application is in communication with said database and configured to authenticate said first portion of said mail identification data by determining whether said first portion of said mail identification data is stored in said database and providing verifying data to said first computer via said network, said verifying data indicating whether said first portion of said mail identification data is stored in said database, wherein at least a portion of said first portion can be used by said mail carrier to identity said sender of said mail object.

See '787 Patent 6:28-6:58.

Claim 30

> 30. A method for authenticating a mail object that includes mail identification data, said mail identification data being 15 encoded into a single barcode, which is then affixed onto said mail object, comprising:
>
> communicating by at least one sender computer at least a first portion of said mail identification data over a network, said mail identification data including a shipping 20 portion including at least shipping method data, a recipient portion including destination data for said mail object, a sender portion, and an identifier portion including at least a numeric value assigned by a sender of said mail object, and said first portion of said mail identification data consisting of said shipping portion, said sender portion and said identifier portion;
>
> receiving by said at least one sender computer verifying data from a second computer via a network, wherein said verifying data verifies the authenticity of said first portion of said mail identification data by stating whether said first portion corresponds to data that is stored on a database in communication with said second computer;
>
> providing said mail object to a mail carrier, wherein at least a portion of said first portion can be used by said mail carrier to identify said sender of said mail object.

See '787 Patent 9:14-36.

Claim 30 Dependent Claims:

> 32. The method of claim 30, wherein said sender portion includes data that is assigned by said mail carrier and can be used to identify a sender of said mail object.

See '787 Patent 9:40-42.

II. Legal Standard

Patent infringement analysis involves two steps: (1) an interpretation of the asserted claims, and (2) a comparison of the claims to the accused device. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 976 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370, 116 S. Ct.

1384 (1996). Claim interpretation is a matter of law, *id*. at 979, and is thus amenable to summary judgment, even though the analysis involves both issues of law and questions of fact. *Phonometrics Inc. v. N. Telecom Inc.*, 133 F.3d 1459, 1463-64 (Fed. Cir. 1998). Many courts, however, have chosen to hold a claim interpretation hearing, or *Markman* hearing, to facilitate the claim interpretation process. *See e.g., Ethicon Endo-Surgery, Inc. v. United States Surgical Corp.*, 93 F.3d 1572, 1577 (Fed. Cir. 1996).

Claim interpretation begins with the language of the claim. *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1324 (Fed. Cir. 2002). Terms in the claim are generally given the ordinary and customary meaning they would have to a person of ordinary skill in the art at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). However, the terms must be read in the context of the entire patent. *Id.* at 1314. In interpreting the claims, the court focuses primarily on the intrinsic evidence of record, including the claims themselves, the specification, and if in evidence, the prosecution history. *Id.* at 1312-17.

Among the intrinsic evidence, the specification is always highly relevant to the claim construction analysis—it is the single best guide to the meaning of a disputed term, and is usually dispositive. *Id.* at 1315 (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)). "The specification is, thus, the primary basis for construing the claims." *Id.* (quoting *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 452 (Fed. Cir. 1985)). In addition to the specification, the court will also consider the prosecution history, consisting of "the complete record" of the patent. *Id*. at 1317. However, because the prosecution history often lacks the clarity of the specification, it is less useful for claim interpretation purposes. *Id.*

While the court may also consider extrinsic evidence, including expert testimony, dictionaries, and learned treatises, as the Federal Circuit has recently made clear, such evidence is generally viewed as less reliable than intrinsic evidence. *Phillips*, 415 F.3d at 1317-18. Therefore, the court must use its discretion in admitting and weighing extrinsic evidence, keeping in mind its inherent flaws. *Id*. at 1319.

III. Claim Construction

The parties request construction of four terms: 1) "sender," and related terms; 2) "recipient" and related terms; 3) "mail verification data" and "verifying data"; and 4) "mail verification device." The Court addresses each in turn.

a. "Sender," "Sender Data," and "Sender Portion"

At the outset, the Court addresses the construction of "sender data," as it is directly defined in each Patent's specifications. The parties agree that "sender data" is indistinguishable from "sender portion" or "sender information." HT2 at 43. "Sender data" is defined in the '268 Patent's specification as "indicating who sent the mail object." '268 Patent 2:32-33; 4:54. In a hearing held before the Board of Patent Appeals and Interferences ("BPAI") on the '268 Patent, the inventor told the Board that "sender data" is defined as "data that can be used to identify the sender." *See* Fitzsimmons Decl. Ex. A-4 at 527. At the final *Markman* hearing, the parties seemed to largely agree on a construction that of "information indicating who the sender is." HT3 at 28. This seems to the Court indistinguishable from the specification definition. The Court therefore adopts the definition provided in the specification, as it is part of the intrinsic evidence and does not appear functionally distinct from the definition given to the BPAI. This also serves as the construction for "sender portion" and "sender information," per the parties' agreement. The Court therefore turns to the parties' greater point of dispute: "sender."

"Sender" is a central term in all of the contested claims. Plaintiff first argued that the Court should construe "Sender" as "any person or entity that is involved in the sending of a mail object to a recipient via a mail carrier." Opp'n at 4. Defendants countered that "sender" is more properly construed with its common dictionary definition as a "person or entity that conveys or causes to be conveyed by an agent, the mail piece." *See* Ds Opp'n to PMSJ at 8. SMS later presented a first alternative construction: "Any person or entity that is involved in the preparation of the mail object for the mail carrier or identified on the mail object as a sender of the mail object." HT2[1] at 24. Defendants preferred this construction, but argued that "sender" should be narrowed to an individual or entity who initiates the content or otherwise

[1] The Court held multiple hearings on this matter, and delineates between the transcripts by using a numeral following "HT." References to the transcript from the first hearing are therefore cited with "HT," from the second hearing with "HT2," and so forth.

commissions the mailing, or an entity that actually packages or handles the mail object itself. *See* HT2 at 36-37. At the final hearing, Plaintiff again revised its position to argue that the sender is "the entity that assigns the unique identifier." HT3 at 10.

The Court concludes that the most accurate construction of "sender," and the only definition identified in the claims or the specifications of the patents, should simply be derived from the "sender data" definition: "who sent the mail object." '268 Patent 2:32-33; 4:54. If the inventor describes "sender data" as "data that can be used to identify the sender," *see* Fitzsimmons Decl. Ex. A-4 at 527, and the specifications identify the same data as "indicating who sent the mail object," the only logical inference is that the "sender" is the person or entity "who sent the mail object." "Sent" should have its common meaning, rather than any specialized definition. "To send" is generically defined as: "To cause to be conveyed by an intermediary to a destination <*send* books to California by train>," or "To dispatch, as by a communications medium <*send* a letter> <*sent* a telegram>," *Merriam Webster New College Dictionary II* 1005 (1995), or, similarly, "To cause to go or be taken to a particular destination, arrange for the delivery of, esp. by mail," *Oxford American Dictionary* 1589 (3d ed. 2010). This is consistent with the clear direction in the claims and the patents' specifications that the sender should be directly associated with the physical mail object in some way.

In reaching this construction, the Court turns first to the claim terms. *Teleflex*, 299 F.3d at 1324. The term is not expressly defined anywhere in the claims. The claim language of the '268 and '787 Patents, however, make clear that the sender assigns the unique identifier that is always included in the mail identification data. *See* '268 Patent 6:25; '787 Patent 5:40. The '787 Patent further states that this value assigned by the sender can be used to identify the sender of the mail object, suggesting that the sender should be somehow associated with the source of the mail object itself. *See* '787 Patent 6:35-60 ("at least a portion of [the mail identification data] . . . can be used by said mail carrier to identify said sender of said mail object."). These two aspects of the "sender" ring true throughout the intrinsic evidence, and support using the construction above.

The specifications of the ‘268 and ‘787 Patents also support using the above construction and the common definition of “to send.” First, each specification suggests a definition of “sender” that requires the sender to be somehow in contact with the mail piece or the source of the mail piece in some way. The specifications define “sender data” as “indicating who sent the mail object,” which suggests that the “sender” is the person or entity “who sent the mail object.” *See* ‘268 Patent 4:45; ‘787 Patent 4:62. There is nothing in either the specifications or claims suggesting that “send” or “sent” means anything other than its plain and ordinary meaning, which further suggests that a sender is one who is directly involved in placing the mail object in the mail stream or directing its placement in the mail stream.

Second, both specifications describe two “problems” that the inventions are designed to mitigate. The first problem is security, and the claimed invention is designed to provide a method of screening mail to prevent exposing recipients to hazardous substances from unknown sources or other unwanted mail. *See* ‘268 Patent 1:30-40; ‘787 Patent 1:32-45. The second problem is that manual delivery “is limited to a one-way production of a finite set of information,” creating problems when “the sender of the mail object is interested in providing or receiving additional information (e.g., product instructions, warranty information, etc.).” ‘268 Patent 1:43-49; ‘787 Patent 1:46-50. The method also allows information that would otherwise have been mailed in hard copy to be sent electronically to reduce costs and the size of the mail object. *See* ‘268 Patent 1:50-55; ‘787 Patent 1:50-59. These purposes are only served if the “sender” is a person or entity who either directed the content of the mailing or was part of the mailing of the physical mail object. Screening packages is only effective if the “sender data” gives the opener some knowledge of where or who the package came from, or what might be in it. Similarly, a person or entity invested in the contents of the mail object or its actual shipment would be much more likely to be concerned about providing product information or reducing shipping costs.

The extrinsic evidence from the prosecution history also supports construing “sender” to require some connection to an entity or person who either directed the content of the mailing or otherwise handled the mail piece. In the BPAI hearing, the inventor made clear that the defining feature of the invention is the ability to use information from the mail object's sender to verify or identify the sender, or the source, of that mail object. The inventor told the Board that "sender data" is defined as "data that can be used to identify the sender." *See* Fitzsimmons Decl. Ex. A-4 at 527. The inventor further explained that the application addressed a "system and method of verifying a mail object" by using data including "a unique identifier that is then *used to identify, or verify, that the mail object came from an identifiable entity*." Fitzsimmons Decl. Ex. A-4 at 517 (emphasis added). The inventor repeated this sentiment again when emphasizing that part of the "claimed invention" is the use of the encoded data "to then verify that the mail object was sent by an identifiable entity." Fitzsimmons Decl. Ex. A-4 at 523.

The Court was initially concerned that there may be some dispute over whether the term "sender" contemplated multiple senders in any given scenario, i.e. that for the purposes of the patented method, there might be an initial party providing the contents for the mailings, a separate party packaging the mail pieces, another party transporting the mail pieces to the post office, and so forth, all of whom could be "senders." At first, the parties agreed that there may be more than one "sender" for any given mail piece. At the final hearing, however, Plaintiff changed its claim construction theory and adopted the position that there could be only one sender for purposes of the method, defined as the individual or entity that assigned the unique identifier. Plaintiff argues that this construction is the most accurate and in fact mandated by the claim terms because the unique identifier is, by definition, assigned by the sender. *See* '268 Patent 6:25. Defendants do not dispute that there could be only one sender, but argue that this construction is redundant.

The Court agrees with the parties that one entity or person serves as the same "sender" for all purposes under the '268 and '787 Patents, although the definition of "sender" allows for a number of types of entities to fulfill that function in any given scenario. The Court disagrees with Plaintiff's proposed construction, however, because it is circular and unsupported by the claims. First, the only definition of sender comes from the definition of "sender data," defined as data "indicating who sent the mail package." This entity identified in the "sender data" must also assign the unique identifier for a method to be covered by the patented claims, but the "sender data" is defined by the conveying of the mail object, not "indicating who assigned the unique identifier." Second, there is simply no suggestion in the claims or specifications that anyone who assigns a unique identifier is a sender for purposes of the patent. All other references to the sender identify it as the source of the mail object or mail contents, not simply the source of the identifier. Indeed, the purposes described in the patents' specifications would not be furthered if the sender were simply the entity that assigned the identifier, but need have no connection to the contents or mailing of the actual mail piece. This would neither allow the recipient to confirm the source of the package for safety reasons, nor help an entity avoid additional shipping challenges. The inventor could have made this distinction vividly clear in the claims and specifications, but chose not to.

It is certainly true that the unique identifier must be assigned by the sender, and that this is a crucial piece of the patented invention. The inventor made it clear at the BPAI hearing that this was a defining aspect of the patent. The inventor specifically distinguished the invention based on this feature, explaining that "the prior art . . . does not teach a situation where a sender provides a non-unique value and you have to concatenate data onto that in order to render a unique value." Fitzsimmons Decl. Ex. A-4 at 525. The inventor stated that one application of the invention was to allow a sender to generate identifying information that was still unique enough to provide tracking, explaining that "the application solves the problem of how do you allow the sender to generate a unique identifier, and they also ensure that that identifier is truly unique enough to track or identify the mail object." Fitzsimmons Decl. Ex. A-4 at 517-518. Furthermore, in response to the BPAI's question, "If I understand what you're saying, is that the distinctive aspect of your invention is this string, single set of encoded data, and that it includes a unique identifier, sender data recipient data, and shipping method data?", the inventor responded, "Correct. Where the unique identifier is generated by the sender, correct." Fitzsimmons Decl. Ex. A-4 at 527; *see also* Fitzsimmons Decl. Ex. A-4 at 528 ("And the unique identifier is assigned by the sender, or, in the specification, it talks about being generated by the sender."). But it does not follow that any assigned unique identifier is assigned by the sender. Rather, there is some pool of entities involved in conveying a mail piece that meet the definition of "sender." How those entities are identified in the encoded data will then determine whether they are, in fact, "senders" infringing on these patents.

Plaintiff objected to Defendants' construction on the grounds that it was inconsistent with the intrinsic evidence and is based solely on extrinsic evidence. Because the Court adopts the Defendants' definition of "send," although not its actual construction, the Court addresses this argument. As discussed above, the common definition of "send" is entirely supported by the intrinsic evidence. All discussions of "sender" in the claims, specification, and history show that a sender must be associated with the contents or physical mail piece involved – they must either cause a certain item to be conveyed (perhaps directing someone else to put out a specific mailing), or convey the object in some way. The definition of "sender data" supports this construction, as do the listed embodiments and the stated purposes for the patent.

The crux of the issue is: any entity that sends a mail piece in the common meaning can be a "sender" within the meaning of the claims. That sender must also be "indicated" in the "sender data." Finally, that sender must have assigned the unique identifier in the mail ID data. Therefore, Plaintiff is correct that for the purposes of this method, the "sender" is the entity that assigns the unique identifier. However, the fact of assigning the unique identifier does not inform whether an entity can qualify as a "sender" for purposes of the patents. Instead, an entity or person who can be considered a "sender" under the patent must be "indicated" by the sender data and must also be the person or entity "who sent the mail object."

The Court concludes that the construing "sender" to be the "person or entity who sent the mail object" is the construction most consistent with the claim language, specifications of the patents, prosecution history, and articulated purpose of the invention.

b. Recipient Data

At the second hearing, the parties stipulated to the following construction: "information indicating who is to receive the mail object, which may include the recipient's address or account number." HT2 at 46. This appears to the Court to be consistent with the claims and specification. Again, the parties do not dispute that "recipient portion" and "recipient information" should have the same construction as "recipient data."

c. “Mail Verification Data” and “Verifying Data”

The parties agree that “mail verification data” and “verifying data” should have the same construction (as distinct from the “verifying portion” of the mail identification data). HT2 at 47. Plaintiff’s final proposed construction is, “data from the sender of the mail object.” Defendants’ final proposed construction is: “data from a mail verification application provided to a reception device if there is correspondence between the verifying portion and the authenticating portion of the mail ID data.” *See* HT2 at 50.

Based on the intrinsic evidence and prosecution history, the Court concludes that “mail verification data” and “verifying data” are properly construed as simply “data from a mail verification application that is provided if there is correspondence between the verifying portion and the authenticating portion of the mail ID data.” The Court declines to import limitations requiring either that the data come from the sender or be sent to the recipient.

From the claims and specification, it is clear that mail verification data is generated when the authenticating and verifying portions of the mail ID correspond. It is also apparent that the mail verification application, which is on the mail ID device, provides the mail verification data. Mail verification data is not actually defined, however. Claim 1 of the ‘268 Patent provides that “mail verification data” is provided “by said computer” via the network “when said authenticating portion of said mail identification data corresponds with said verifying portion of said mail identification data.” ‘268 Patent 6:34-37. Claims 11 through 15 of the ‘268 Patent describe the method of Claim 1, but provide variations on the content and destination of the mail verification data. ‘268 Patent at 7:15-31.

In the “Background of the Invention” in the ‘268 Patent, the invention is described as “a system and method of authenticating at least one mail object by providing at least a portion of mail identification data over a wide area network, such as the internet, in order to receive mail verification data.” ‘268 Patent at 1:16-19. The detailed description explains that the mail verification application is part of the mail ID device, and the mail verification application stores the verifying portion of the mail ID data, receives the authenticating portion of the mail ID data from the reception device, and provides the mail verification data if the authenticating portion is authenticated (i.e. corresponds). *See* ‘268 Patent 3:35-42. This description is echoed in the description of another embodiment, describing the mail verification application running on the mail ID device as comparing the authenticating portion of the mail ID with the stored verifying portion. If there is correspondence, “then mail verification data is sent to the reception device.” ‘268 Patent 4:38-44. The detailed description further suggests one possible embodiment in which the mail verification data could include authenticating data, securing data (showing who secured the mail object), sender data, or recipient data. *See* ’268 Patent 4:45-58.

There are no requirements for the content of the mail verification data. The specification provides that it may include recipient data, sender data, securing data (“indicating who secured the mail object”), or additional data including instructions, product data, third party advertisements, etc. *See* ‘268 Patent 2:30-35. Thus, although the claims use the term “verifying data,” the specification is clear that the actual information need not confirm anything specific about the package’s contents or sender, and need not provide any particular information about the package’s origins. Mail verification data can serve either of the two enumerated purposes of the ‘268 Patent: ensuring or verifying the package’s source or contents for safety reasons, or providing information that might otherwise have required physical mailing.

The first dispute the Court must address is whether the construction should include a destination. Defendants argue that the mail verification data must go to a reception device or a recipient. *See* HT2 at 57-58. This limitation seems improper, however, in light of claims 11 through 15, which designate different destinations for the mail verification data, including “at least one reception device” (claim 11), and “a recipient” (claim 13). These claims are dependent claims of Claim 1, suggesting that Claim 1 is broader than either of these two requirements. Although the preferred embodiments specify that the mail verification data should be sent to the reception device, Claim 13 contains the limitation of the verification data being sent to a recipient. Claims 11 and 13 are dependent claims to Claim 1, and so the limitation it provides cannot apply to all claims. *See Phillips*, 415 F.3d at 1315. Furthermore, the inventor removed exactly this limitation from his application during prosecution for reasons that are not explained. *See* Fitzsimmons Decl. Ex. A-4 at 346. It would be improper to read such a limitation back into the patent after it has been expressly removed. *Laryngeal Mask Co. Ltd. v. Ambu*, 618 F.3d 1367, 1372 (Fed. Cir. 2010).

In addition to the question whether mail verification data must go to a specific entity or location, the parties also dispute whether mail verification data must come *from* a sender. Although the Court was initially inclined to agree that mail verification data could be construed to come from a sender, this construction does not actually appear supported in the claim or specification language. The more accurate description seems to be to describe the verification data as coming from the mail verification application upon correspondence between the verifying and authenticating ID portions; there is no language in the claims or specification that would suggest the verification data comes only from the sender.

Indeed, the specification suggests that mail verification data could include information that has nothing to do with the sender. For example, the Summary of the Invention states that the mail verification data could include securing data ("indicating who secured the mail object"), and/or sender data, clearly suggesting that the "securing" and "sending" parties could be different individuals. It would make sense for securing data to come from a securing party separate from the sender, especially if the securing party confirmed the contents' safety, inspection, or secure transport. Similarly, the Summary considers the possibility that the mail verification data may include "third party advertisements," which appear by definition to originate not with the sender. These details also appear in the description of the preferred embodiment. *See* '268 Patent 4:52-58. Finally, the description of the preferred embodiment describes one embodiment in which the mail verification data includes "software-booting data adapted to boot an email application and/or a browser application," either one of which could be used to "receive additional information from either the mail ID device, the sender of the mail object, or a third party." *See* '268 Patent 5:35-41. This further suggests that the mail verification data is not exclusively in the purview of the sender.

Because there is no indication in the claims that the mail verification data comes from the sender, the only basis to associate this data with the sender appears to be through the mail ID or verification devices. Mail verification data is produced by the mail verification application, which resides on the mail ID device, which Plaintiffs argue is controlled or operated by the sender. Leaving aside for now whether the mail ID device is so controlled, it seems unnecessary and outside the actual claims and specification to attribute any origin to the mail verification data itself. It further appears, based on the above discussion, that even if the data were generated by a device controlled by the sender, the content or data provided might be from a different entity. The Court therefore declines to read a limitation into the claims that appears unsupported in the patents. Plaintiff elaborates on this point by arguing that “the sender that generated the mail ID data is the one who can ‘verify’ or ‘authenticate’ the mail ID data.” Even if the Court were to accept this argument, it does not follow that the data produced after verification or authentication is necessarily from the sender itself. Indeed, the actual data may not “verify” or “authenticate” anything about the piece, but instead acts as a confirmation of “correspondence” that can take many forms.

The experts on each side do little to clarify this question. Dr. Lopresti opines that the term should be construed as “data from an authorized sender,” Lopresti Decl. ¶¶ 102-03, but there is nothing in the claim language or specification that explains how the Court should construe “authorized sender.” Dr. Allais opines that the “mail verification data” is “data transmitted by the Mail Identification Device.” Allais Decl. ¶¶ 43-45. Dr. Allais further opines that the “mail identification device” is “associated with a location where the mail originates.” Allais Decl. ¶¶ 26-32. Again, this does not suggest a need to import any further limitation to the “mail verification data.”

The Court understands the common sense appeal of assuming that all verifying data will be “from” the sender in some sense. This appears to be the intent of the preferred embodiments, and makes intuitive sense. On the other hand, the inventor presented the patents as defined by the sender-generated unique identifier, which is specifically identified as such in the patent. It was possible for the inventor to also define mail verification data as being generated, assigned, or otherwise from the sender, but there is no such limitation. It also appears to the Court that there are possible embodiments for which the verifying data is not from the sender, possibly in the embodiment involving an independent security institute or a government office.

The Court is therefore inclined to construe “mail verification data” and “verifying data” as simply “data from a mail verification application that is provided if there is correspondence between the verifying portion and the authenticating portion of the mail ID data.”

d. Mail Verification Device

The term “mail verification device” is not used in the ‘268 Patent until Claim 33, and is used again in Claim 52. No definition is provided in the specification or claims. The mail verification device appears to play the same role that the mail ID device plays in Claim 1, and this is the position Plaintiff adopts. Plaintiff argues that “mail verification device,” and thus by extension mail ID device, should be construed as a “device operated by a sender of the mail object.” Defendants respond that the mail verification device (and thus mail ID device) should not be construed as “sender operated.” Based on the claim language and specification, the Court concludes that the mail verification device is: “a device adapted to communicate with one or more reception devices via a network, comprised of at least a memory and a mail verification application adapted to store the verifying portion of mail ID data, receive the authenticating portion of mail ID data, and provide mail verification data.” The Court sees no basis in the claims or specification of the ‘268 Patent for narrowing this construction further, or importing a “sender-operated” limitation.

Turning first to the claims and specification, the Court notes that “mail verification device” has no explicit definition. The fullest description is in Claim 33 of the ‘268 Patent, which provides:

> 33. A mail verification system for authenticating at least one mail object . . . comprising:
>
> at least one mail verification device adapted to communicate with at least one reception device via a network, said at least one mail verification device comprising:
>
> a memory; and
>
> a mail verification application adapted to:
>
> store at least a verifying portion of mail identification data in said memory . . . ;

> receive at least an authenticating portion of said mail identification data from said at least one reception device via said network . . . ; and
>
> provide mail verification data via said network . . .

'268 Patent 8:62-9:19. The description and figures make clear that it is the device that hosts the mail verification application, and so is the device that receives data from the reception device to determine whether there is "correspondence." In a colloquial sense, it is the device or computer at the front end of the process of verifying a mail object – storing a piece of data that will later be compared to the data sent from the scanner or other form of reception device where the mail object arrives. This reinforces that the mail verification device and the mail ID device perform the same basic function.

The only indications Plaintiff cites for the mail ID device and mail verification device being "sender operated" are expert opinions and statements made by the inventor during prosecution. The inventor's statements, however, appear to discuss one possible embodiment, not all possible embodiments. *See* Fitzsimmons Decl. Ex. A-4 at 402-403 ("In *one embodiment* of the present invention, a sender uses a mail ID device . . .") ("The specification further provides that a sender *can* use a mail ID device (110) or more particularly, a mail verification application (112) operating thereon . . .") (emphasis added). Defendants' expert opines that the mail verification device "would logically be the same as the Mail Identification Device" because the mail verification application resides on the mail ID device. *See* Allais Decl. ¶ 42. Plaintiff's expert writes that "the mail verification device is used by a sender of the mail object," but does not opine further. *See* Sterling Rebuttal Decl. ¶ 36.

Both experts opine more fully on the meaning of "mail identification device." Defendants' expert looks to the common specification and notes that the mail ID device is "associated with a location where the mail originates." Allais Decl. ¶ 31. Plaintiff's expert opines that the mail ID device "is described in the common specification as being used by a sender of the mail object." Sterling Rebuttal ¶ 21. Sterling further supports this position with a statement made by the inventor during the prosecution history ("a sender can use a mail ID device (110), or more particularly, a mail verification application (112) operating thereon, to generate the mail ID data (or a portion thereof)." Sterling Rebuttal Decl. ¶ 21. The inventor also stated that the mail ID device could be used to compare received data to stored data, possibly "to determine whether a mail object was sent from a secure location or an authorized (or at least an identifiable) entity." Sterling Rebuttal Decl. ¶ 21. Based on this evidence, Sterling opined that "the mail ID device is associated with a sender of the mail object, and more particularly, is used by a sender of the mail object to store, receive and compare mail ID data, or a portion thereof." Sterling Rebuttal ¶ 22.

Although the Court understands the intuitive appeal of reading a "sender-operated" limitation into the claim language, this does not seem supported by the patent itself. The references to a sender operating the mail ID device or mail verification device are not mandatory; they are rather iterations of the invention or the preferred embodiment. The claims themselves are broader. The claims and specification in fact appear to run against a "sender operated" limitation. First, the '268 Patent specifically associates the unique identifier with the sender, showing that the inventor could have specified that the mail ID device or mail verification device were also specifically related to the sender. *See* '268 Patent 6:24-26 (". . . wherein said unique identifier consists of a numeric value assigned by a sender of said at least one mail object.").

Second, there are several proposed embodiments in which the sender and the mail ID device are entirely separate, further suggesting that the mail ID device cannot be construed to *always* be sender-operated. *See* '268 Patent 5:29-35 ("Either one of these applications could then be used to . . . provide additional information to said mail ID device (or the sender of the mail object), and/or receive additional information from either the mail ID device, the sender of the mail object, or a third-party."); '268 Patent 5:35-41 ("In another embodiment, the mail verification data further includes software-booting data adapted to boot an email application and/or a browser application. Either one of these applications could then be used to provide additional information to the mail ID device and/or receive additional information from either the mail ID device, the sender of the mail object, or a third party."); '268 Patent 5:42-49 ("In another embodiment of the invention, the reception device 120, or more particularly the mail authenticating application 122 is adapted to provide a reply email to the mail ID device 130 *or the sender* of the mail object. This reply email may either be sent automatically . . . or manually, to allow the recipient to communicate with the mail ID device *and/or* sender of the mail object.") (emphasis added). Thus, because the claims and specification contain no language limiting the mail verification device or mail ID device to a sender's control, and the specification in fact suggests embodiments in which the sender and mail ID device are contacted separately, the Court declines to read this limitation into the '268 Patent. This leaves open the question of how the mail verification device should in fact be construed.

From this, the Court concludes that the mail verification device is simply defined by its terms in the claims: "a device adapted to communicate with one or more reception devices via a network, comprised of at least a memory and a mail verification application adapted to store the verifying portion of mail ID data, receive the authenticating portion of mail ID data, and provide mail verification data." The Court sees no basis in the claims or specification of the '268 Patent for further describing a mail verification device or narrowing this construction.

IV. Disposition

The Court hereby adopts the foregoing claim constructions for the claims at issue. The Court will issue a separate order on the motions for summary judgment.

DATED: April 8, 2014

David O. Carter

DAVID O. CARTER
UNITED STATES DISTRICT JUDGE